Web Results **1 - 10** of about **26** for **gpu + encryption + video card + "cryptographic processor"**. (**0.31** second

Methods and systems for cryptographically protecting secure ...
A method according to claim 1, wherein the **cryptographic processor** is ... at least one command buffer sent to a **video** decode unit of the at least one **GPU** ...
www.patentstorm.us/patents/7203310-claims.html - 38k - Cached - Similar pages

Microsoft Windows and industryand operating system Resources on ...
Tags: **Video** cards, Operating systems, Semiconductors, adjustment, **video card**, monitoring, hardware, clock speed, AGP, graphics, Microsoft Windows, chipset, ...
search.techrepublic.com.com/search/Microsoft+Windows+and+industry+and+operating+system.html - 69k - Cached - Similar pages

processor and **video card** Resources on TechRepublic
Tags: **GPU**, Columbia University, graphics, cryptography, **video card**, processor ... Authentication/**Encryption**, Digital security, smart **card**, authentication ...
search.techrepublic.com.com/search/processor+and+**video+card**.html?t=13&s=0&o=0 - 49k - Supplemental Result - Cached - Similar pages
[More results from search.techrepublic.com.com]

Methods and systems for authentication of components in a graphic ...
a graphics **card** having at least one **GPU** and a **cryptographic processor** ..... Figures 9A and 9B are block diagrams illustrating exemplary **encryption** ...
www.freepatentsonline.com/EP1355218.html - 125k - Cached - Similar pages

Methods and systems for authenticationof components in a graphics ...
A computing device, comprising: one of an application and device; and a graphics **card** having at least one **GPU** and a **cryptographic processor** communicatively ...
www.freepatentsonline.com/20030200435.html - 126k - Cached - Similar pages
[More results from www.freepatentsonline.com]

Electrical Computers And Digital Processing Systems: Support ...
In a plurality of storage systems including data **encryption** functions, ... In one embodiment, data that is stored in memory other than a **video card** ...
www.freshpatents.com/x1713189000psbc.php - 121k - Cached - Similar pages

[PDF] Trusted Computing.ppt
File Format: PDF/Adobe Acrobat
GPU. Multi. IO. Multi. IO. 64 MB. Memory. USB 1.1. **Video**. Encoder ..... **Cryptographic Processor**. RSA Engine (**encryption** and digital signatures) ...
https://www.blackhat.com/presentations/win-usa-04/bh-win-04-blight/bh-win-04-blight.pdf - Similar pages

$FreeBSD: src/share/misc/pci_vendors,v 1.34 2005/07/18 07:43:35 ...
File Format: Unrecognized - View as HTML
... Millennium P650 Series 4536 Meteor 2 STD/MC/Dig **Video** Capture **Card** 6573 ..... 001D 7956 **Cryptographic Processor** 0020 7954/7955 **Cryptographic Processor** ...
cvsup.pt.freebsd.org/cgi-bin/cvsweb/cvsweb.cgi/src/share/misc/pci_vendors?rev=1.34 - Similar pages

[PDF] *EP001355218A2*
File Format: PDF/Adobe Acrobat - View as HTML
authenticating a graphics **card** in connection with a sys- ... having **GPU**(s) and a **cryptographic processor** communicatively and securely coupled to the **GPU**(s), ...
https:/.../PublicationServer/documentpdf.jsp?iDocId=5427427&iebug=.pdf - Supplemental Result - Similar pages

pci_vendors
NVIDIA **GPU** Quadro FX 4500 2679 00A0 RIVA TNT2 Aladdin [NVA0] 2680 00B4 ..... 001D 7956 **Cryptographic Processor** 5775 0020 7954/7955 **Cryptographic Processor** ...
opengrok.creo.hu/dragonfly/xref/src/share/misc/pci_vendors - 705k -
Cached - Similar pages

1 2 **Next**

Terms used: **gpu cryptography video card cryptographic processor**

Found **9,671** of **206,720**

Sort results by: publication date
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 141 - 160 of 200 Result page: previous 1 2 3 4 5 6 7 **8** 9 10 next
Best 200 shown Relevance scale

141 SoftGenLock: active stereo and genlock for PC cluster

Jérémie Allard, Valérie Gouranton, Guy Lamarque, Emmanuel Melin, Bruno Raffin
May 2003 **Proceedings of the workshop on Virtual environments 2003 EGVE '03**
Publisher: ACM Press

Full text available: pdf(1.10 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we present SoftGenLock, an open source software that enables genlock and active stereo on commodity graphics cards. SoftGenLock is implemented on top of Linux. It does not require any hardware modification of the graphics card. Rather than to gain total control on signal generation, which would make the software deeply dependent on the graphics card specification, SoftGenLock applies continuous small modifications to converge and maintain genlocked video signals. To be properly sy ...

Keywords: Genlock, PC cluster, active stereo, immersive projection environment, real-time

142 Session 4: big stuff: Interactive visibility culling in complex environments using occlusion-switches

Naga K. Govindaraju, Avneesh Sud, Sung-Eui Yoon, Dinesh Manocha
April 2003 **Proceedings of the 2003 symposium on Interactive 3D graphics I3D '03**
Publisher: ACM Press

Full text available: pdf(2.03 MB) Additional Information: full citation, abstract, references, cited by, index terms

We present occlusion-switches for interactive visibility culling in complex 3D environments. An occlusion-switch consists of two GPUs (graphics processing units) and each GPU is used to either compute an occlusion representation or cull away primitives not visible from the current viewpoint. Moreover, we switch the roles of each GPU between successive frames. The visible primitives are rendered in parallel on a third GPU. We utilize frame-to-frame coherence to lower the communication overhead be ...

Keywords: conservative occlusion culling, interactive display, levels-of-detail, multiple GPUs, parallel rendering

143 Optimizing the energy consumed by secure wireless sessions: wireless transport layer security case study
Ramesh Karri, Piyush Mishra
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(151.69 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we identified the various sources of energy consumption during the setup, operation and tear down of a secure wireless session by considering the wireless transport layer security protocol. Our analysis showed that data transfers during a secure wireless transaction, number and size of messages exchanged during secure session establishment and cryptographic computations used for data authentication and privacy during secure data transactions in that order are the main sources of en ...

Keywords: WTLS, energy-efficient, mobile, secure session, security, wireless

144 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration
Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(107.24 KB) Additional Information: full citation, abstract, references, index terms

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, that is the MS, actually the SIM, the visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS and the UMTS architecture carry the heritage of the GSM's philosophy regarding the user/network authentication and the data ciphe ...

Keywords: PKIs, PLMNs, asymmetric cryptography

145 Securing Mobile Appliances: New Challenges for the System Designer
Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(257.28 KB) Publisher Site Additional Information: full citation, abstract, citings, index terms

As intelligent electronic systems pervade all aspects of our lives, capturing, storing, and communicating a wide range of sensitive and personal data, security is emerging as a critical concern that must be addressed in order to enable several current and future applications. Mobile appliances, which will play a critical role in enabling the visions of ubiquitous computing and communications, and ambient intelligence, are perhaps the most challenging to secure ¿ they often rely on a public mediu ...

146 Masking the Energy Behavior of DES Encryption
H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, W. Zhang
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(264.41 KB)

Publisher Site Additional Information: full citation, abstract, citings, index terms

Smart cards are vulnerable to both invasive and non-invasive attacks. Specifically, non-invasive attacks using power and timing measurements to extract the cryptographic key has drawn a lot of negative publicity for smart card usage. The power measurement techniques rely on the data-dependent energy behavior of the underlying system. Further, power analysis can be used to identify the specific portions of the program being executed to induce timing glitches that may in turn help to bypass key ch ...

147 On-line e-wallet system with decentralized credential keepers

Stig Frode Mjølsnes, Chunming Rong
February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1
Publisher: Kluwer Academic Publishers
Full text available: pdf(240.23 KB) Additional Information: full citation, abstract, references, index terms

We propose a generalization of the architecture of an electronic wallet, as first developed in the seminal European research project CAFE. With this model you can leave most of the content of your electronic wallet at the security of your residential electronic keeper, while roaming with your favorite mobile terminals. Emerging mobile handsets with both short range Bluetooth and cellular GPRS communications provide a sufficient communication platform for this electronic wallet architecture. Howe ...

Keywords: digital credentials, e-wallet architecture, mobile commerce, payment protocols, privacy

148 Leading edge design examples: Design of a scalable RSA and ECC crypto-processor

Ming-Cheng Sun, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu
January 2003 **Proceedings of the 2003 conference on Asia South Pacific design automation ASPDAC**
Publisher: ACM Press
Full text available: pdf(127.33 KB) Additional Information: full citation, abstract, references, citings

In this paper, we propose a scalable word-based crypto-processor that performs modular multiplication based on modified Montgomery algorithm for finite fields *GF(P)* and *GF*(2^m). The unified crypto-processor supports scalable keys of length up to 2048 bits for RSA and 512 bits for elliptic curve cryptography (ECC). Further extension of the key length can be done easily by enlarging the memory module or using the external memory resource. With the proposed parity pre ...

149 Cryptographic protocols: The verification of an industrial payment protocol: the SET purchase phase

Giampaolo Bella, Lawrence C. Paulson, Fabio Massacci
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**
Publisher: ACM Press
Full text available: pdf(209.87 KB) Additional Information: full citation, abstract, references, citings, index terms

The Secure Electronic Transaction (SET) protocol has been proposed by a consortium of credit card companies and software corporations to secure e-commerce transactions. When the customer makes a purchase, the SET dual signature guarantees authenticity while keeping the customer's account details secret from the merchant and his choice of goods secret from the bank.This paper reports the first verification results for the complete purchase phase of SET. Using Isabelle and the inductive method, we ...

Keywords: electronic commerce, formal verification, inductive specifications, isabelle proof assistant, security protocols

150 Crytography: Generic implementations of elliptic curve cryptography using partial reduction

Nils Gura, Hans Eberle, Sheueling Chang Shantz
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**
Publisher: ACM Press
Full text available: pdf(216.56 KB) Additional Information: full citation, abstract, references, index terms

Elliptic Curve Cryptography (ECC) is evolving as an attractive alternative to other public-key schemes such as RSA by offering the smallest key size and the highest strength per bit. The importance of ECC has been recognized by the US government and the standards bodies NIST and SECG. Standards for preferred elliptic curves over prime fields GF(p) and binary polynomial fields GF(2^m) as well as the Elliptic Curve Digital Signature Algorithm (ECDSA) have been created. A security protoco ...

Keywords: elliptic curve cryptography, modular reduction

151 Simulation and architecture evaluation: Using modern graphics architectures for general-purpose computing: a framework and analysis

Chris J. Thompson, Sahngyun Hahn, Mark Oskin
November 2002 **Proceedings of the 35th annual ACM/IEEE international symposium on Microarchitecture MICRO 35**
Publisher: IEEE Computer Society Press
Full text available: pdf(1.07 MB) Publisher Site Additional Information: full citation, abstract, references, citings, index terms

Recently, graphics hardware architectures have begun to emphasize versatility, offering rich new ways to programmatically reconfigure the graphics pipeline. In this paper, we explore whether current graphics architectures can be applied to problems where general-purpose vector processors might traditionally be used. We develop a programming framework and apply it to a variety of problems, including matrix multiplication and 3-SAT. Comparing the speed of our graphics card implementations to stand ...

152 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

153 Practical experiences: Security-driven exploration of cryptography in DSP cores

Catherine H. Gebotys
October 2002 **Proceedings of the 15th international symposium on System Synthesis ISSS '02**
Publisher: ACM Press
Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, index terms

With the popularity of wireless communication devices a new important dimension of embedded systems design has arisen, that of security. This paper presents for the first time design exploration for secure implementation of cryptographic applications on a complex DSP processor core. A new metric for security, the implementation security index, is introduced for measuring resistance to power attacks. Elliptic curve cryptographic algorithms are used to demonstrate and quantize security, energy, pe ...

Keywords: DSP, low energy, methodology, power analysis attack

154 Special session on security on SoC: Securing wireless data: system architecture challenges

Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally
October 2002 **Proceedings of the 15th international symposium on System Synthesis ISSS '02**
Publisher: ACM Press
Full text available: pdf(172.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of current and future wireless data applications and services. This paper highlights the challenges posed by the need for security during system architecture design for wireless handsets, and provides an overview of emerging techniques to address them. We focus on the computational requirements for securing wireless data transactions, revealing a gap between these requirements and the trends in processing capabilities of embedded processors used in wireless h ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, WTLS, decryption, design methodology, embedded system, encryption, handset, mobile computing, performance, platform, security, security processing, system architecture, wireless communications

155 Special session on security on SoC: Special session: security on SoC

Cathy Gebotys, Hiroto Yasuura, Michael Torla, Srivaths Ravi, Naofumi Takagi
October 2002 **Proceedings of the 15th international symposium on System Synthesis ISSS '02**
Publisher: ACM Press
Full text available: pdf(238.87 KB) Additional Information: full citation, abstract, references

SoC is one of the important components of social and personal information systems, which directly influence with our life, property and privacy. Security technology is now embedded into various hardware and software of SoC and SoC designers should be concerned with security issues. Cryptography requires heavy computation and wireless communication requests architecture and protocols for security. In design process of SoC, choice of IP's and design data control also significantly affect on the se ...

156 Enabling trusted software integrity

Darko Kirovski, Milenko Drinić, Miodrag Potkonjak
October 2002 **ACM SIGPLAN Notices , ACM SIGARCH Computer Architecture News , ACM SIGOPS Operating Systems Review , Proceedings of the 10th international conference on Architectural support for programming**

languages and operating systems ASPLOS-X, Volume 37 , 30 , 36 Issue 10 , 5 , 5
Publisher: ACM Press
Full text available: pdf(1.39 MB) Additional Information: full citation, abstract, references, citings

Preventing execution of unauthorized software on a given computer plays a pivotal role in system security. The key problem is that although a program at the beginning of its execution can be verified as authentic, while running, its execution flow can be redirected to externally injected malicious code using, for example, a buffer overflow exploit. Existing techniques address this problem by trying to detect the intrusion at run-time or by formally verifying that the software is not prone to a p ...

157 Ray tracing on programmable graphics hardware
Timothy J. Purcell, Ian Buck, William R. Mark, Pat Hanrahan
July 2002 **ACM Transactions on Graphics (TOG) , Proceedings of the 29th annual conference on Computer graphics and interactive techniques SIGGRAPH '02**, Volume 21 Issue 3
Publisher: ACM Press
Full text available: pdf(454.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Recently a breakthrough has occurred in graphics hardware: fixed function pipelines have been replaced with programmable vertex and fragment processors. In the near future, the graphics pipeline is likely to evolve into a general programmable stream processor capable of more than simply feed-forward triangle rendering.In this paper, we evaluate these trends in programmability of the graphics pipeline and explain how ray tracing can be mapped to graphics hardware. Using our simulator, we analyze ...

Keywords: programmable graphics hardware, ray tracing

158 Development of processors and communication networks for embedded systems: System design methodologies for a wireless security processing platform
Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally, Murugan Sankaradass
June 2002 **Proceedings of the 39th conference on Design automation DAC '02**
Publisher: ACM Press
Full text available: pdf(207.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Security protocols are critical to enabling the growth of a wide range of wireless data services and applications. However, they impose a high computational burden that is mismatched with the modest processing capabilities and battery resources available on wireless clients. Bridging the security processing gap, while retaining sufficient programmability in order to support a wide range of current and future security protocol standards, requires the use of novel system architectures and design m ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, decryption, design methodology, embedded system, encryption, handset, performance, platform, security, security processing, system architecture, wireless

159 Processors and accelerators for embedded applications: Unlocking the design secrets of a 2.29 Gb/s Rijndael processor
Patrick R. Schaumont, Henry Kuo, Ingrid M. Verbauwhede
June 2002 **Proceedings of the 39th conference on Design automation DAC '02**
Publisher: ACM Press
Full text available: pdf(329.22 KB) Additional Information: full citation, abstract, references, citings, index terms

This contribution describes the design and performance testing of an Advanced Encryption Standard (AES) compliant encryption chip that delivers 2.29 GB/s of encryption throughput at 56 mw of power consumption. We discuss how the high level reference specification in C is translated into a parallel architecture. Design decisions are motivated from a system level viewpoint. The prototyping setup is discussed.

Keywords: Rijndael, domain-specific, encryption, low-power

160 Computer security: Implementation of fast RSA key generation on smart cards

Chenghuai Lu, Andre L. M. dos Santos, Francisco R. Pimentel
March 2002 **Proceedings of the 2002 ACM symposium on Applied computing SAC '02**
Publisher: ACM Press

Full text available: pdf(645.79 KB) Additional Information: full citation, abstract, references, citings, index terms

Although smart cards are becoming used in an increasing number of applications, there is small literature of the implementation issues for smart cards. This paper describes the issues and considerations that need to be taken into account when implementing the key generation step of a cryptographic algorithm widely used nowadays, RSA.Smart cards are used in many applications that require a tamper resistant area. Therefore, smart cards that use cryptography have to provide encryption, decryption, ...

Keywords: RSA key generation, coprocessor, prime finding, smart card